



---

## Cechy rozwiązania

- Rozpoznawanie i ograniczenie ryzyka utraty danych w punktach końcowych (na stacjach roboczych).
  - Skuteczniejsze zapobieganie niewłaściwemu wykorzystaniu danych poprzez monitorowanie, nadzór i blokowanie działań.
  - Ograniczenie zaangażowania ekspertów klienta na etapach planowania, implementacji i bieżącej eksploatacji rozwiązania.
- 

# Usługi IBM w dziedzinie ochrony danych w punktach końcowych

## *Oprogramowanie Verdasys Digital Guardian*

### Ochrona danych, która nie utrudnia pracy zespołowej

Istnieje szereg środków technicznych umożliwiających trudne do wykrycia wyniesienie danych z sieci firmowej – użytkownicy mogą użyć w tym celu laptopów z nagrywarkami płyt CD i DVD, drukarek, urządzeń typu Blackberry, pamięci flash (pendrive), poczty elektronicznej z interfejsem WWW, a także sieci bezprzewodowych. Nawet gdy dane objęte szczególną ochroną znajdują się w środowisku nadzorowanym, może dojść do ich ujawnienia lub naruszenia. Dlatego organizacje muszą dysponować mechanizmami zapewniającymi widoczność informacji i przejrzystość operacji na danych, aby skutecznie je chronić przed utratą i niewłaściwym wykorzystaniem.

IBM, biorąc pod uwagę powyższe problemy, oferuje obecnie najlepsze w swojej klasie rozwiązanie zapobiegające utracie danych, przeznaczone do ochrony w punktach końcowych sieci. Stanowi ono połączenie oprogramowania Verdasys Digital Guardian ze specjalnie skonstruowanym pakietem usług IBM w dziedzinie ochrony danych. Oprogramowanie Verdasys Digital Guardian jest kompleksowym rozwiązaniem do automatycznego wykrywania i klasyfikacji wrażliwych danych na stacjach roboczych i serwerach oraz do monitorowania danych w trakcie ich przesyłania i wykorzystania. Ponadto oprogramowanie może w sposób zautomatyzowany stosować mechanizmy zabezpieczające niezbędne do ochrony danych. Rozwiązanie przyczynia się do skutecznej implementacji firmowych strategii i polityk bezpieczeństwa oraz ogranicza ryzyko utraty danych.

### Spójne egzekwowanie wewnętrznych i prawnie wymaganych strategii bezpieczeństwa

Przedsiębiorstwa, w których kluczowe znaczenie ma ochrona newralgicznych danych, potrzebują strategii zapobiegania utracie danych w punktach końcowych oraz zintegrowanego rozwiązania umożliwiającego:

- Wykrywanie i klasyfikację danych.
- Centralne zarządzanie strategiami.
- Adekwatne do poziomu ryzyka reagowanie na naruszenia strategii.
- Zautomatyzowane mechanizmy kontrolne.
- Powiązanie działań z generowanymi alertami i raportami.
- Zapewnienie globalnej przejrzystości wykorzystania i położenia danych.



### Strategia ochrony informacji skoncentrowana na danych, a nie na systemach

Rozwiązanie IBM zapobiegające utracie danych w punktach końcowych pomaga w monitorowaniu i zabezpieczeniu przepływu newralgicznych danych w przedsiębiorstwie. Oprogramowanie Digital Guardian działa w miejscach, w których dane są faktycznie wykorzystywane, w czasie rzeczywistym stosuje odpowiednie mechanizmy ochrony. Klient z pomocą IBM może zaimplementować platformę zabezpieczającą punkty końcowe, której działanie zorientowane jest na ochronę danych. Menedżerowie odpowiedzialni za sferę biznesową i informatyczną mogą używać takiego rozwiązania do:

- Wykrywania i klasyfikowania danych objętych szczególną ochroną na podstawie kontekstu i treści,
- Oceny ryzyka udostępniania danych objętych szczególną ochroną i podejmowania na tej podstawie decyzji biznesowych oraz budowania strategii bezpieczeństwa.
- Stosowania mechanizmów ochrony danych w punktach końcowych w sposób zgodny z przyjętymi strategiami, pozwalając przypisać odpowiedzialność użytkownikom końcowym i sprzyjając dobrowolnemu przestrzeganiu zasad bezpieczeństwa.
- Zapobiegania utracie danych w sposób niezakłócający pracy zespołowej i wymiany informacji.

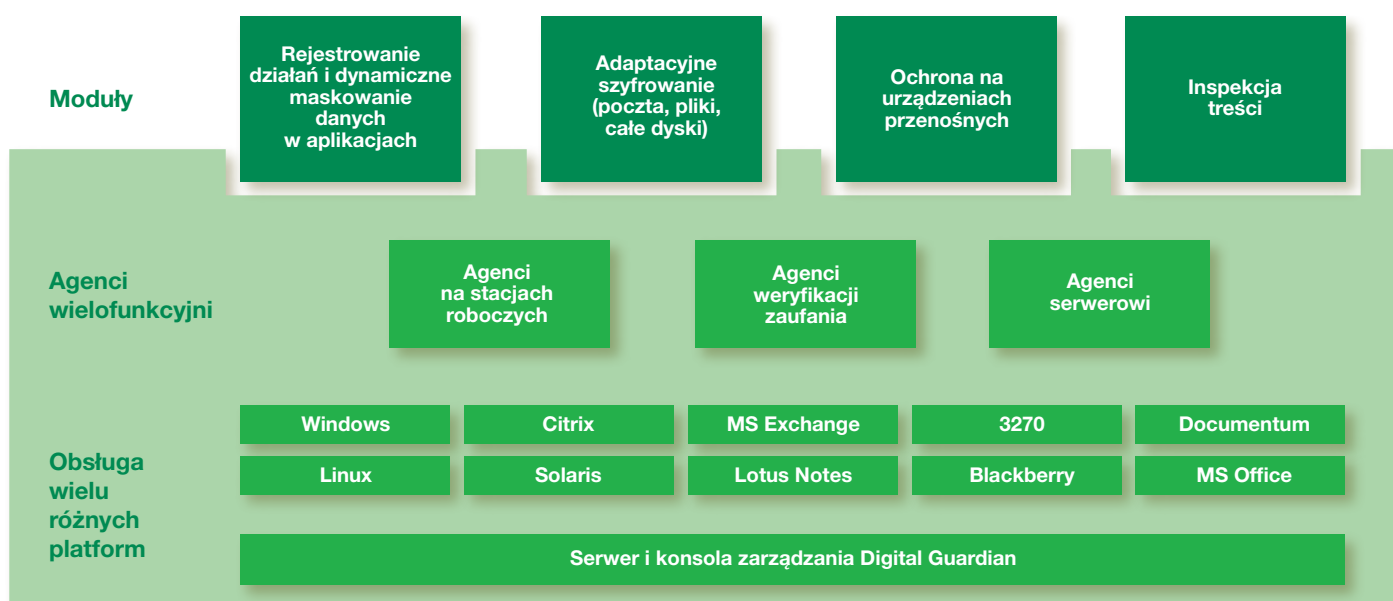
Rozwiązanie IBM zapobiegające utracie i wypływowi danych w punktach końcowych może monitorować, rejestrować działania, ostrzegać, szyfrować dane, a w razie potrzeby blokować niedozwolone czynności użytkowników końcowych na stacjach roboczych, laptopach i serwerach (wewnątrz organizacji i poza nią).



### Aktywny nadzór nad wykorzystaniem informacji objętych szczególną ochroną

Oprogramowanie Verdasys Digital Guardian umożliwia kontrolę nad dostępem do informacji objętych szczególną ochroną, a jednocześnie nadzoruje i aktywnie kontroluje ich wykorzystanie. Rozwiązanie to zapewnia:

- Wszelkierne ochronę danych realizowaną zarówno w sieci korporacyjnej, jak i poza nią.
- Ogólnokorporacyjną widoczność położenia i wykorzystania danych objętych szczególną ochroną oraz pomoc w podejmowaniu decyzji operacyjnych.
- Scentralizowane definiowanie i egzekwowanie strategii obejmujących nie tylko weryfikację tożsamości i działań, lecz także klasyfikację danych na podstawie ich kontekstu i treści.



- Adekwatne do ryzyka i zgodne z przyjętą strategią reakcje na działania użytkowników, w tym ostrzeżenia, blokady i alerty oraz zautomatyzowane szyfrowanie plików i wiadomości e-mail.

### Ochrona danych tam, gdzie są używane

Rozwiązania IBM oraz oprogramowanie Verdasys Digital Guardian zapewniają ochronę przed ujawnieniem lub utratą danych w całym przedsiębiorstwie, oferując takie możliwości, jak:

- **Wykrywanie i klasyfikacja danych** – utworzone strategię klasyfikacji danych są egzekwowane przez bezpieczne, niewidoczne oprogramowanie w punktach końcowych, w oparciu o kombinację klasyfikacji na podstawie kontekstu i treści.
- **Monitorowanie ruchu danych i działań użytkowników** – agenci na podstawie kontekstu i treści monitorują oraz rejestrują wszystkie działania użytkowników obejmujące interakcje z plikami, siecią, schowkiem, drukarkami, podsystemami napędów CD.
- **Zautomatyzowane stosowanie adekwatnych do ryzyka mechanizmów kontrolnych** – agenci, w oparciu o klasyfikację i analizę operacji na danych stosują odpowiednie mechanizmy kontrolne, takie jak ostrzeżenia, monitory, wymóg uzasadnienia operacji, zautomatyzowane szyfrowanie lub nawet zablokowanie transakcji na danych, zanim użytkownik narazi informacje na zagrożenie.
- **Szyfrowanie plików** – automatyczne, zgodne z przyjętą strategią szyfrowanie plików objętych szczególną ochroną na dyskach lokalnych stacji roboczych, a także na pamięciach zewnętrznych i nośnikach CD/DVD.
- **Szyfrowanie poczty elektronicznej** – opatentowana technika szyfrowania treści i załączników wiadomości e-mail; działa automatycznie zgodnie z przyjętą strategią oraz obejmuje zarządzanie kluczami szyfrowania. Zintegrowany mechanizm szyfrowania poczty elektronicznej egzekwuje strategię bezpieczeństwa w sieci oraz w systemach poczty z interfejsem WWW.
- **Rejestrowanie działań i maskowanie w aplikacjach** – kontrola dostępu na poziomie pól danych realizowana poprzez ich maskowanie, spełniająca formalne wymogi dotyczące zapisów kontrolnych w starszych aplikacjach (z emulatorem terminala 3270), aplikacjach klient-serwer i aplikacjach z interfejsem WWW.
- **Raporty kontrolne i wspomagające podejmowanie decyzji** – wszechstronne funkcje raportowania udostępniające zagregowane raporty zawierające informacje o wykorzystaniu danych w przedsiębiorstwie, raportowanie trendów, raporty grupowe i indywidualne, raporty o „danych w spoczynku”, raporty o zgodności ze strategiami oraz raporty operacyjne.

- **Badanie danych w postaci elektronicznej i raporty na potrzeby postępowań dowodowych** – zagregowane raporty ze spraw zawierające informacje o wykorzystaniu danych w całym przedsiębiorstwie, w tym o działaniach realizowanych bez połączenia z siecią (offline), działaniach podwykonawców i partnerów.

### Jak w pełni wykorzystać potencjał rozwiązania?

Usługi oferowane przez IBM pomagają w pełnym wykorzystaniu potencjału rozwiązania do ochrony danych w punktach końcowych. Usługi te uwzględniają wyzwania, jakie wiążą się z wdrożeniem każdego złożonego rozwiązania – takie jak kontrola kosztów i zakresu prac, sprawna implementacja oraz ograniczenie zaangażowania kadrowego. Oferta IBM obejmuje m.in. następujące usługi:

- **Warsztaty służące określeniu wymagań i opracowaniu planu wdrożenia**  
Identyfikacja danych objętych szczególną ochroną i ryzykownych aplikacji oraz mierzenie wpływu ujawnienia danych na prowadzoną działalność.
- **Oszacowanie potrzeb w zakresie ochrony danych**  
Ma na celu zdefiniowanie strategii zapobiegania utracie danych oraz priorytetów wdrożenia i testowania.
- **Implementacja i projektowanie strategii**  
Planowanie projektu, architektury i strategii, testowanie komponentów, testowanie przedprodukcyjne, pomoc w wdrożeniu i transfer wiedzy w fazie implementacji.

### Dlaczego IBM i Verdasys?

IBM i Verdasys, Inc. wspólnie oferują kompleksowe, wiarygodne i transparentne rozwiązanie zapewniające ochronę danych w punktach końcowych. Klienci mogą z pełnym zaufaniem wdrażać oprogramowanie Verdasys Digital Guardian, mając do dyspozycji zaplecze merytoryczne i usługowe działu IBM Global Technology Services. Usługa IBM do ochrony danych w punktach końcowych, oparte na oprogramowaniu Verdasys, obejmuje najlepsze rozwiązanie techniczne, strategiczne doradztwo, analizę ryzyka, usługi wdrożeniowe i zarządzanie rozwiązaniem.

## Więcej informacji

Aby uzyskać więcej informacji o usługach IBM w dziedzinie ochrony danych w punktach końcowych oraz oprogramowaniu Verdasys Digital Guardian, należy skontaktować się z przedstawicielem IBM, Partnerem Handlowym IBM lub odwiedzić stronę [www.ibm.com/services/pl](http://www.ibm.com/services/pl)

[ibm.com/services/pl](http://www.ibm.com/services/pl)

Ponadto IBM Global Financing może zaproponować rozwiązania finansowe dostosowane do konkretnych potrzeb informatycznych klienta. Więcej informacji na temat atrakcyjnych stawek, elastycznych planów spłat, kredytów oraz usług odkupu i zagospodarowania zasobów można znaleźć pod adresem: [ibm.com/financing/pl](http://www.ibm.com/financing/pl)



© Copyright IBM Corporation 2011

IBM Polska Sp. z o.o.  
ul. 1 Sierpnia 8  
02-134 Warszawa  
tel. (+ 48 22) 878 67 77  
faks (+ 48 22) 878 68 88

Strona główna IBM znajduje się pod adresem:  
[ibm.com/pl/](http://www.ibm.com/pl/)

Wyprodukowano w Polsce  
Styczeń 2011  
Wszelkie prawa zastrzeżone

IBM, logo IBM i [ibm.com](http://www.ibm.com) są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach. Jeśli powyższe nazwy oraz inne nazwy znaków towarowych IBM oznaczone zostały przy ich pierwszym wystąpieniu w tym tekście symbolem znaku towarowego (® lub ™), oznacza to, że w chwili opublikowania tej informacji znaki te były zarejestrowane w Stanach Zjednoczonych przez IBM lub były własnością IBM z mocy powszechnie obowiązującego prawa. Takie znaki towarowe mogą być również zarejestrowane w innych krajach lub podlegać warunkom powszechnie obowiązującego tam prawa. Aktualna lista znaków towarowych IBM dostępna jest w serwisie WWW IBM, w sekcji „Copyright and trademark information” (Informacje o prawach autorskich i znakach towarowych), pod adresem [ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

Nazwy innych firm, produktów lub usług mogą być znakami towarowymi lub znakami usług innych firm. Zawarte w niniejszej publikacji odniesienia do produktów lub usług firmy IBM nie oznaczają, że IBM zamierza udostępnić je we wszystkich krajach, w których działa.

Klient ponosi odpowiedzialność za przestrzeganie przepisów prawnych. Do obowiązków Klienta należy uzyskanie porady kompetentnej kancelarii prawnej w zakresie wskazania odpowiednich przepisów i ich interpretacji, które mogą mieć wpływ na prowadzoną przez Klienta działalność. Klient jest również odpowiedzialny za wszelkie inne działania, które winien podjąć w celu zapewnienia takiej zgodności. IBM nie zapewnia porad prawnych oraz nie dokonuje ustaleń ani nie gwarantuje, że usługi czy produkty IBM zapewnią zgodność działań przedsiębiorstwa Klienta z przepisami.